the Committee on Agriculture, Nutrition, and Forestry.

By Mr. McCLURE (by request):

S. 2285. A bill to promote competition in the natural gas market, to ensure open access to transportation service, to encourage production of natural gas, to provide natural gas consumers with adequate supplies at reasonable prices, to eliminate demand restraints, and for other purposes; to the Committee on Energy and Natural Resources.

By Mr. DECONCINI:

S. 2286. A bill to prohibit the sale, donation, or other transfer of STINGER antiaircraft missiles to democratic resistence forces in Afghanistan and Angola unless certain conditions are met; to the Committee on Foreign Relations.

By Mr. BRADLEY (for himself and Mr. LAUTENBERG):

S. 2287. A bill to amend the Wild and Scenic Rivers Act to designate a certain portion of the Great Egg Harbor River in the State of New Jersey for potential addition to the wild and scenic rivers system; to the Committee on Energy and Natural Resources.

SUBMISSION OF CONCURRENT AND SENATE RESOLUTIONS

The following concurrent resolutions and Senate resolutions were read, and referred (or acted upon), as indicated:

By Mr. ABDNOR (for himself, Mr. NICKLES, Mr. SYMMS, Mr. MCCLURE, Mr. ANDREWS, Mr. BOREN, Mr. HECHT, Mr. GORE, Mr. DURENBERGER, Mr. BOSCHWITZ, Mr. HEFLIN, Mr. DENTON, Mr. ARMSTRONG, Mrs. HAWKINS, and Mrs. KASSEBAUM):

S. Res. 379. A resolution to express the sense of the Senate that the Secretary of Agriculture should take certain actions to minimize the adverse effect of the milk production termination program on beef, pork, and lamb producers, and for other purposes; to the Committee on Agriculture, Nutrition, and Forestry.

By Mr. LAUTENBERG (for himself and Mr. WEICKER):

S. Res. 380. A resolution expressing the sense of the Senate of the United States of America that the United States Government should not undertake any efforts to interfere with the free market by encouraging OPEC or its members to adopt production controls to artificially raise oil prices; to the Committee on Foreign Relations.

By Mr. DECONCINI:

S. Res. 381. A resolution expressing the sense of the Senate with respect to United States corporations doing business in Angola; to the Committee on Banking, Housing, and Urban Affairs.

STATEMENTS ON INTRODUCED BILLS AND JOINT RESOLUTIONS

By Mr. WILSON (for himself, Mrs. HAWKINS, Mr. MCCLURE, Mr. HEFLIN, Mr. SYMMS, Mr. ABDNOR, Mr. GRASSLEY, Mr. WALLOP, Mr. DECONCINI, and Mr. SIMPSON):

S. 2280. A bill to amend the Agricultural Act of 1949 to suspend the application of the milk production termination program in order to minimize the adverse effect of the program on beef, pork, and lamb producers; to the Committee on Agriculture, Nutrition, and Forestry.

(The remarks of Mr. WILSON and the text of the legislation appear earlier in today's RECORD.)

By Mr. TRIBLE (for himself, Mr. LAXALT, Mr. DENTON, Mr. ARMSTRONG, and Mr. DIXON):

S. 2281. A bill to amend title 18, United States Code, to provide additional penalties for fraud and related activities in connection with access devices and computers, and for other purposes; to the Committee on the Judiciary.

COMPUTER FRAUD AND ABUSE ACT

Mr. TRIBLE. Mr. President, I am introducing today a revised version of legislation I sponsored last year to combat computer crime. I am especially pleased that the chairman of the Criminal Law Subcommittee, Senator LAXALT, has joined me in sponsoring this bill, along with Senators DENTON, ARMSTRONG, and DIXON. Congressman HUGHES is introducing identical legislation today in the House of Representatives.

This new bill will supersede S. 440, the computer crime legislation I introduced in February of 1985. That measure was the subject of a hearing before the Criminal Law Subcommittee on October 30, 1985. In the months since, I have worked closely with Senator LAXALT to meet the concerns raised at that hearing, and I believe that this new bill will adequately address the computer crime problems facing the Federal Government, federally insured financial institutions, and the private sector.

In general, this measure will expand the protections against computer crime currently enjoyed by the Federal Government. Likewise, new offenses will be created for theft or intentional destruction of computer data when the offense is committed on an interstate basis, or when the crime is committed against computers belonging to federally insured financial institutions. Trafficking in computer passwords by those who intend to defraud the owner of the subject computer will also be proscribed.

The advent of widespread computer use has brought a great many benefits to the Nation. This Congress must act to ensure that those benefits are protected against computer criminals. I believe this legislation will do so, and I urge my colleagues to join Senator LAXALT and me in cosponsoring this bill.

I also ask unanimous consent that detailed analysis of the legislation and a copy of the bill itself appear in the RECORD at this point.

There being no objection, the material was ordered to be printed in the RECORD, as follows:

S. 2281

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "Computer Fraud and Abuse Act of 1986".

SEC. 2. SECTION 1030 AMENDMENTS.

(a) MODIFICATION OF DEFINITION OF FINANCIAL INSTITUTION.—Section 1030(a)(2) of title 18, United States Code, amended—

(1) by striking out "knowingly" and inserting "intentionally" in lieu thereof; and

(3) by striking out "as such terms are defined in the Right to Financial Privacy Act of 1978 (12 U.S.C. 3401 et seq.),".

(b) MODIFICATION OF EXISTING GOVERNMENT COMPUTERS OFFENSE.—Section 1030(a)(3) of title 18, United States Code, is amended—

(1) by striking out "knowingly" and inserting "intentionally" in lieu thereof;

(2) by striking out ", or having accessed" and all that follows through "prevents authorized use of, such computer";

(3) by striking out "It is not an offense" and all that follows through "use of the computer." and

(4) by striking out "if such computer is operated for or on behalf of the Government of the United States and such conduct affects such operation;" and inserting in lieu thereof "if such computer is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, if such computer is used by or for the Government of the United States and such conduct affects such use".

(c) MODIFICATION OF AUTHORIZED ACCESS ASPECT OF OFFENSES.—Paragraphs (1) and (2) of section 1030(a) of title 18, United States Code, are each amended by striking out ", or having accessed" and all that follows through "does not extend" and inserting "or exceeds authorized access" in lieu thereof.

(d) NEW OFFENSES.—Section 1030(a) of title 18, United States Code, is amended by inserting after paragraph (3) the following:

"(4) knowingly and with intent to defraud, accesses a Federal interest computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer;

"(5) intentionally accesses a Federal interest computer without authorization, and by means of one or more instances of such conduct alters information in that computer, or prevents authorized use of that computer, and thereby causes loss to another of a value aggregating $1,000 or more during any one year period; or

"(6) knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information through which a computer may be accessed without authorization, if—

"(A) such trafficking affects interstate or foreign commerce; or

"(B) such computer is used by or for the Government of the United States;".

(e) ELIMINATION OF SECTION SPECIFIC CONSPIRACY OFFENSE.—Section 1030(b) of title 18, United States Code, is amended—

(1) by striking out "(1)"; and

(2) by striking out paragraph (2).

(f) PENALTY AMENDMENTS.—Section 1030 of title 18, United States Code, is amended—

(1) by striking out "of not more than the greater of $10,000" and all that follows through "obtained by the offense" in subsection (c)(1)(A) and inserting "under this title" in lieu thereof;

(2) by striking out "of not more than the greater of $100,000" and all that follows through "obtained by the offense" in subsection (c)(1)(B) and inserting "under this title" in lieu thereof;

(3) by striking out "or (a)(3)" each place it appears in subsection (c)(2) and inserting ", (a)(3) or (a)(6)" in lieu thereof;

(4) by striking out "of not more than the greater of $5,000" and all that follows through "created by the offense" in subsection (c)(2)(A) and inserting "under this title" in lieu thereof;

(5) by striking out "of not more than the greater of $10,000" and all that follows through "created by the offense" in subsection (c)(2)(B) and inserting "under this title" in lieu thereof;

(6) by striking out "not than" in subsection (c)(2)(B) and inserting "not more than" in lieu thereof,

(7) by striking out the period at the end of subsection (c)(2)(B) and inserting "; and" in lieu thereof; and

(8) by adding at the end of subsection (c) the following:

"(3)(A) a fine under this title or imprisonment for not more than five years, or both, in the case of an offense under subsection (a)(4) or (a)(5) of this section which does not occur after a conviction for another offense under such subsection, or an attempt to commit an offense punishable under this subparagraph; and

"(B) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(4) or (a)(5) of this section which occurs after a conviction for another offense under such subsection, or an attempt to commit an offense punishable under this subparagraph.".

(g) CONFORMING AMENDMENTS TO DEFINITIONS PROVISION.—Section 1030(e) of title 18, United States Code, is amended—

(1) by striking out the comma after "As used in this section" and inserting a one-em dash in lieu thereof;

(2) by aligning the remaining portion of the subsection so that it is cut in two ems and begins as an indented paragraph, and inserting "(1)" before "the term";

(3) by striking out the period at the end and inserting a semicolon in lieu thereof; and

(4) by adding at the end thereof the following:

"(2) the term 'Federal interest computer' means a computer—

(A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects such use; or

"(B) which is one of two or more computers used in committing the offense, not all of which are located in the same State;

"(3) the term 'State' includes the District of Columbia, the Commonwealth of Puerto Rico, and any other possession or territory of the United States;

"(4) the term 'financial institution' means—

"(A) a bank with deposits insured by the Federal Deposit Insurance Corporation;

"(B) the Federal Reserve or a member of the Federal Reserve including any Federal Reserve Bank;

"(C) an institution with accounts insured by the Federal Savings and Loan Insurance Corporation;

"(D) a credit union with accounts insured by the National Credit Union Administration;

"(E) a member of the Federal home loan bank system and any income loan bank; and

"(F) any institution of the Farm Credit System under the Farm Credit Act of 1971;

"(5) the term 'financial record' means information derived from any record held by a financial institution pertaining to a customer's relationship with the financial institution; and

"(6) the term 'exceeds authorized access' means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter.".

(h) LAW ENFORCEMENT AND INTELLIGENCE ACTIVITY EXCEPTION.—Section 1030 of title 18, United States Code, is amended by adding at the end the following new subsection:

"(f) This section does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States.".

ANALYSIS—COMPUTER FRAUD AND ABUSE ACT OF 1986

This legislation will expand somewhat the types of criminal miconduct involving computers that will be subject to federal jurisdiction. However, I intend, together with the cosponsor of this bill, that the federal role be expanded only to those areas where there is a compelling federal interest in the prevention and punishment of computer crimes. To that end, this bill provides additional protections against computer crimes affecting the Federal Government itself and federally insured financial institutions; it also proscribes some types of computer crimes that are interstate in nature.

AMENDMENTS TO PRESENT LAW

At present, 18 USC 1030(a)(1) provides for punishement of thefts by computer of national security-related information. This is a felony offense and will remain so. This bill will alter that provision of law only to the extent necessary to simplify the language pertaining to those who "exceed authorized access" to a particular computer system.

The same change will be made to present 18 USC 1030(a)(2). In addition, 18 USC 1030(a)(2) will be altered by changing the scienter requirement from "knowingly" to "intentionally". I am concerned that a "knowingly" standard, when applied to computer use and computer technology, might not be sufficient to preclude liability on the part of those who inadventently "stumble into" someone else's computer file. This is particularly true with respect to those who are authorized to use a particular computer, but subsequently exceed their authorized access by entering another's computer file. It is not difficult to envision a situation in which an authorized computer user will mistakenly enter someone else's computer file. Because the user had "knowingly" signed onto the computer in the first place, the danger exists that he might incur liability for his mistaken access to another file. The substitution of an "intentional" standard is meant to focus federal criminal prosecutions under this paragraph on those who evince a clear intent to enter, without authorization, computer files belonging to another.

The premise of 18 USC 1030(a)(2) remains the protection, for privacy purposes, of computerized information relating to customers' relationships with financial institutions. I believe strongly that the protection offered consumer reporting agency's in the 1984 computer crime legislation must be preserved. This was a valuable addition to the federal criminal statutes, and it ought not be reduced or eliminated. But this bill will also extend those privacy protections to the financial records of all customers—individual and corporate—of financial institutions, as defined in this new bill. As under present law, a first offense under this subsection will be punishable as a misdemeanor. Felony penalties will be available for second and subsequent offenses.

This legislation will also clarify the present 18 USC 1030(a)(3), making clear that it applies to acts of simple computer trespass against computers belonging to, or being used by or for, the Federal government. The Department of Justice and others have expressed concerns about whether present law covers mere trespass offenses, or whether it requires a further showing that the information perused was "used, modified, destroyed, or disclosed." To alleviate those concerns, this legislation will make clear that 18 USC 1030(a)(3) is a trespass offense, applicable to those outside the Federal government. Those government employees who lack the requisite authorization to use a particular computer, or who merely exceed their authorized access can be dealt with in an administrative manner, rather than by criminal punishment. This should alleviate concerns that first arose in 1984 about access and use by whistle-blowers of government-related information that was stored in a computer. So too was deletion of the "disclosure" portion of 18 USC 1030(a)(3). The intentional modification or destruction of computerized information belonging to the government will be covered by a different provision of this proposal. As with 18 USC 1030(a)(2), the scienter requirement in this paragraph will be changed from "knowingly" to "intentionally". A first offense under this subsection will be a misdemeanor; second and subsequent offenses will be felonies.

While the provision of present law relating to attempted offenses will remain unchanged, the provision relating to conspiracies (18 USC 1030(b)(2)) will be deleted entirely. Conspiracies to commit computer crimes wil be treatable under the general federal conspiracy statute, 18 USC 371.

NEW OFFENSES

The new paragraph (a)(4) to be created by this bill is aimed at penalizing thefts of property via computer that occur as part of a scheme to defraud. It will require a showing that the use of the computer or computers in question was integral to the intended fraud, and was not merely incidental. To trigger this provision, the property obtained by the offender in wrongfully accessing a particular computer must further the intended fraud, and not be superfluous to it. The mere use of a computer for recordkeeping purposes, for example, is not meant to constitute an offense under this provision. The use of a computer by one who has devised a scheme to defraud should constitute an offense only when the computer was used to obtain property of another which furthers the fraud, or when the use can be shown to constitute an attempted crime under this chapter.

This paragraph is designed in part, to help distinguish between acts of theft via computer and acts of computer trespass. In intentionally trespassing into someone else's computer files, the offender obtains at the very least information as to how to break into that computer system. If that is all he obtains, the offense should properly be treated as a simple trespass. But because the offender has obtained the small bit of information needed to get into the computer system, the danger exists that his and every other computer trespass could be treated as a theft, punishable as a felony. I do not believe this is a proper approach to this problem. There must be a clear distinction between computer theft, punishable as a felony, and computer trespass, punishable as a misdemeanor. The element in the new

paragraph (a)(4), requiring a showing of an intent to defraud, is meant to preserve that distinction, as is the requirement that the property wrongfully obtained via computer furthers the intended fraud. Offenses under this subsection will be treatable as felonies.

The new paragraph (a)(5) is a malicious mischief statute, and is designed to provide penalties for those who intentionally damage or destroy computerized data belonging to another. Such damage may include an act intended to alter another's computer password, thereby denying him access to his own computerized information. It will be necessary, in proving this offense, that the government demonstrate that a loss has been incurred by the victim totaling at least $1,000 in a single year. This is necessary to prevent the bringing of felony-level malicious mischief charges against every individual who modifies another's computer data. Some modifications, while constituting "damage" in a sense, do not warrant felony-level punishment, particularly when they require almost no effort or expense to repair. The $1,000 evaluation is reasonably calculated to preclude felony punishment in those cases, while preserving the option of felony punishment in cases involving more serious damage or destruction. In instances where the requisite dollar amount cannot be shown, misdemeanor-level penalties will remain available against the offender under the trespass statute created by this bill. Thus, the valuation will not exist for determining the presence or absence of federal jurisdiction; it will serve instead to help determine whether the act constituting the offense is punishable as a felony or a misdemeanor.

In addition, the concept of "loss" embodied in this paragraph will not be limited solely to the cost of actual repairs. The Justice Department has suggested that other costs, including the cost of lost computer time necessitated while repairs are being made, be permitted to count toward the $1,000 valuation. I and the other sponsors of this bill agree.

Finally, in new paragraph (a)(6), this bill provides penalties for those who, knowingly and with an intent to defraud, traffic in computer passwords belonging to others. If those elements are present—and if the password in question would enable unauthorized access to a government computer, or if the trafficking affects intrastate or foreign commerce—this provision could be invoked. A first offense under this subsection will constitute a misdemeanor; second and subsequent offenses will constitute felonies.

● Mr. LAXALT. Mr. President, the legislation being introduced today by Senator TRIBLE and Congressman HUGHES represents a cooperative effort to tighten up the existing statute, 18 U.S.C. 1030, and to propose several new criminal offenses that appear to be necessary at this time. The Committee on the Judiciary has already scheduled a hearing on this bill, and I would hope that the committee will report the measure to the full Senate in the near future.

Rather than repeat Senator TRIBLE's excellent analysis of the bill, I would like simply to focus on the new fraud and malicious mischief offenses and indicate what we are trying to achieve in those two sections. (Proposed 18 U.S.C. 1030(a)(4) and (a)(5).)

The acts of "fraud" that we are addressing in proposed section 1030(a)(4) are essentially thefts in which someone uses a Federal interest computer to wrongly obtain something of value from another. We intend that the use of the computer be an integral—not merely an incidental—part of the commission of the theft.

By including the element of "intent to defraud" in the offense, we wish to distinguish between true theft offenses, where obtaining something of value is the intended object of the act, from the acquisition of knowledge or information that is often incidental to a simple act of unauthorized access.

Computer crime brings into sharp focus the fact that information is a valuable commodity and must be considered property that can be stolen. It is also true that persons who commit acts of unauthorized access often complete those transactions in possession of more knowledge, and hence more information or property, than they had before the act, even though the taking of the information was not the intended object of their offense.

Proposed section 1030(a)(4) is intended to reflect the distinction between theft of information, a felony, and mere unauthorized access, a misdemeanor.

The malicious mischief offense, proposed section 1030(a)(5), contains a jurisdictional amount of at least $1,000 in losses in a 1-year period. In light of the disdain of the Department of Justice for jurisdictional amounts— a disdain that I generally share—I want to make clear that the purposes of the $1,000 loss element are: First, to distinguish between alterations that should fairly be treated as misdemeanors and those that should be felonies; and second, to limit Federal jurisdiction to the felonious alterations. Setting a specific loss value is one way to achieve this end, though it may not be the best one.

The issues raised by computer crime and computer crime legislation are often subtle and exceedingly difficult to solve. Senator TRIBLE and Congressman HUGHES have struggled mightily—and, I believe, successfully—to solve many of those problems in this bill. I know that they welcome the good counsel and advice of all interested parties on these issues as the Congress considers this important legislation.●

By Mr. DOLE for Mrs. HAWKINS:

S. 2282. A bill to establish a national advanced technician training program utilizing the Nation's eligible colleges to expand and improve the supply of technicians required by industry and national security in strategic, advanced, and emerging technology in order to increase the productivity of the Nation's industries, to contribute to the self-sufficiency of competitiveness of the United States in international trade, and for other purposes; to the Committee on Labor and Human Resources.

NATIONAL ADVANCED TECHNICIAN TRAINING ACT

● Mrs. HAWKINS. Mr. President, the American economy and the American work force today face global challenges of unprecedented scale. The key to meeting these challenges lies in large measure in skill training, in expanding the pool of technicians employed at the cutting edge of new and changing industrial technology. The legislation I introduce today, the National Advanced Technician Training Act, addresses this need.

The essence of this bill, Mr. President, is partnerships. Community and technical colleges already have gone further than any other segment of higher education in building programs tailored to the needs of employers and the private sector.

Yet the employer community is just one of many populations knocking at the community college doors. The community colleges serve larger minority populations than any other segment of higher education. Almost 45 percent of the total black community in higher education is attending community colleges; 70 percent of the Hispanic community is tackling its college dreams through community colleges. The community colleges also are serving a more recent phenoomenon in higher education—the so-called reverse transfers. In the State of Washington, among others, the students moving from senior institutions back to community colleges, in order to satisfy the demands of the workplace, are greater in number than the enrollments transferring from the community colleges into the universities and senior colleges.

Growing numbers of adults who already hold higher college degrees—BA's through Ph.D.'s—are using the community colleges to meet the changing skill needs of their careers. For reasons of convenience and economy, the community colleges are the colleges of choice of the innumerable single parents and displaced homemakers who are striving to gain new or better employment. Such diverse demands from the community are putting a severe strain on the budgets of most community colleges. They simply lack the budgetary resources to increase their outreach to employers, and to instigate the courses that will more fully serve the accelerating changes of the workplace. With the seed support that my bill proposes, Mr. President, the partnerships between industry and community colleges that address the emerging priorities of high technology can be encouraged and expanded far beyond their present scope.

In the emerging workplace, Mr. President, virtually all occupations—from auto mechanic, draft and design technician, and machinist to nurse and secretary—require the worker to be prepared in the competencies of high technology. For the nurse and medical technician, it means working with electronically controlled life support systems and exotic lifesaving pharmaceuticals. For the draftsman it means working with computer-aided design,